UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/627,017 | 07/25/2003 | John Mendonca | 200209600-1 | 3688 |

22879 7590 02/13/2009
HEWLETT PACKARD COMPANY
P O BOX 272400, 3404 E. HARMONY ROAD
INTELLECTUAL PROPERTY ADMINISTRATION
FORT COLLINS, CO 80527-2400

| EXAMINER | |
|---|---|
| OKORONKWO, CHINWENDU C | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2436 | |

| NOTIFICATION DATE | DELIVERY MODE |
|---|---|
| 02/13/2009 | ELECTRONIC |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

JERRY.SHORMA@HP.COM
mkraft@hp.com
ipa.mail@hp.com

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

## BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/627,017
Filing Date: July 25, 2003
Appellant(s): MENDONCA ET AL.

John P. Wagner Jr.
For Appellant

## EXAMINER'S ANSWER

This is in response to the appeal brief filed 11/17/2008 appealing from the Office action mailed 08/05/2008.

### (1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

### (2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board’s decision in the pending appeal.

### (3) Status of Claims

The statement of the status of claims contained in the brief is correct.

### (4) Status of Amendments After Final

The appellant’s statement of the status of amendments after final rejection contained in the brief is correct.

### (5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

### (6) Grounds of Rejection to be Reviewed on Appeal

The appellant’s statement of the grounds of rejection to be reviewed on appeal is correct.

### (7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

### (8) Evidence Relied Upon

| | | |
|---|---|---|
| US Patent No. 6,578,147 | Shanklin et al. | June 10, 2003 |

### (9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

### *Claim Rejections - 35 USC § 102*

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

Claims 1-20 are rejected under 35 U.S.C. 102(e) as being disclosed by Shanklin et al. (U.S. Patent No. 6,578,147 B1).

Regarding claims 1, 8 and 15, Shanklin et al., discloses a method, system and a computer readable medium comprising computer-executable instructions stored therein for managing utilization of network intrusion detection systems in a dynamic data center, said method comprising: providing a plurality of network intrusion detection systems, each being networked so that utilization of each network intrusion detection system can be based on demand for said network intrusion detection systems in said dynamic data center (column 2 lines 48-50 – “Multiple intrusion detection sensors are used at the entry point to the network, specifically, at an ‘internetworking device’ such as a router or a switch” and column 2 lines 54-58 – “Internetworking device, whether a router or switch, is processor-based and includes load balancing programming, which controls how packets are distributed from the internetworking device to the sensors for processing”); receiving a monitoring policy and a plurality of monitoring points to be monitored on a network with any of said network intrusion detection systems (column 2 lines 1-13 – Shanklin et al. discloses the claimed “monitoring policy” as being inclusive to the IDS sensors, which comprise: “packet load to the sensors that is ‘load balanced’, such that said packets are distributed at least at a session-based level [or] packet-based level … the results of the detection performed by the sensors and the network analyzer are used to determine if there is an attempt to gain unauthorized access to the network”); and automatically arranging the monitoring of said monitoring points using said network intrusion detection systems and said monitoring policy (column 5 lines 19-20 – Shanklin et al. again discloses the “monitoring points” as being inclusive to the IDS sensors, which comprise “load balancing unit, which distributes packet among the sensors,” which can be “session-based (column 5 line 22)" or “network-based (column 5 line 58)").

> Shanklin et al. recites intrusion detection sensors which "autonomously comprise the entire intrusion detection system (column 3 lines 58-62). Therefore, the Examiner understands the disclosed "multiple intrusion detection sensors" to comprise the function of claimed plurality of network intrusion detection system, monitoring points and monitoring policy. Thus the disclosure of Shanklin et al. highlights the various elements and components of the disclosed "multiple intrusion detection sensors are used at the entry point to the network, specifically, at an 'internetworking device' such as a router or a switch."

Regarding claims 2, 9 and 16, Shanklin et al., discloses a method, system and a computer readable medium comprising computer-executable instructions stored therein for automatically arranging the monitoring of said monitoring points includes: automatically configuring a plurality of network resources to provide network communication data from said monitoring points to a plurality of available network intrusion detection systems from said network intrusion detection systems (column 3 lines 59-65 – "[sensors] might forward alarms to station 10c, which may then alert the sytem manager or automatically take action"); and automatically configuring said available network intrusion detection systems to receive said network communication data based on said monitoring policy (column 2 lines 1-7 – "packet load to the sensors that is 'load balanced', such that said packets are distributed at least at a session-based level [or] packet-based level … the results of the detection performed by the sensors and the network analyzer are used to determine if there is an attempt to gain unauthorized access to the network).

Regarding claim 3, Shanklin et al., discloses a method, system and a computer readable medium comprising computer-executable instructions stored therein for automatically arranging the monitoring of said monitoring points further includes: automatically increasing a number of particular network intrusion detection systems receiving said network communication data from a particular monitoring point by selecting additional available network intrusion detection systems if said network communication data exceeds a capacity of said particular network intrusion detection systems (column 2 lines 1-18 and column 3 lines 57-65 – the claimed automatically increasing IDS systems is found in the disclosure of the "solution provided by the invention [being] easily scalable" in size from large scale to small scale).

Regarding claims 4, 11 and 18, Shanklin et al., a method, system and a computer readable medium comprising computer-executable instructions stored therein for automatically arranging the monitoring of said monitoring points further includes: automatically decreasing a number of particular network intrusion detection systems receiving said network communication data from a particular monitoring point by releasing any of said particular network intrusion detection systems to said available network intrusion detection systems if said network communication data is below a predetermined threshold of a capacity of said particular network intrusion detection systems (column 2 lines 1-18 and column 3 lines 57-65 – the claimed automatically decreasing IDS systems is found in the disclosure of the “solution provided by the invention [being] easily scalable” in size from large scale to small scale

Regarding claims 5, 12 and 19, Shanklin et al., discloses a method, system and a computer readable medium comprising computer-executable instructions stored therein for which resources include one of a firewall, a gateway system, a network switch, and a network router (column1 lines 19-28 or column 3 lines 23-29).

Regarding claims 6 and 13, Shanklin et al., discloses a method, system and a computer readable medium comprising computer-executable instructions stored therein for receiving a monitoring policy and a plurality of monitoring points to be monitored includes: providing a graphical user interface to receive said monitoring policy and said plurality of monitoring points to be monitored (column 3 lines 54-57 – “user interface”).

Regarding claims 7, 14, 20, Shanklin et al., discloses a method, system and a computer readable medium comprising computer-executable instructions stored therein for which dynamic data center is a utility data center (column 1 lines 19-26).

**(10) Response to Argument**

**A. Rejection of Claims 1-20 under 35 USC § 102(e).**

In response to Applicant argument that the Shanklin reference does not teach or suggest a dynamic system that receives "a monitoring policy and a plurality of monitoring points to be monitored," the Examiner respectfully disagrees, submitting that the although the Applicant argues Shanklin's supposed lack of support for "a dynamic system," nowhere in the claim language is there mention of a dynamic system. Instead the claim language contains the limitations mentioning of only a dynamic data center which "automatically arrang[es] the monitoring of said monitoring points using said network intrusion detection systems and said monitoring policy." The Examiner first submits that what makes this data center (later claimed as a *system* in claim 15) dynamic is the automatic arranging or assigning of received packets to monitoring points using the IDS and monitoring (security) policy. Further the Examiner emphasizes that the "real time" intrusion detection system of the Shanklin disclosure does indeed read upon this claim limitation as it first discloses the well known process of receiving a monitoring or security policy from a network administrator in the recitation of a firewall or server being “configured by the administrator of the local network based on the enterprise's security policy (1:19-26).” Secondly, Shanklin continues by providing an example of how this policy would function, reciting, "the firewall [or server] may block traffic of a certain type, traffic from certain addresses, or traffic from all but a predetermined set of addresses … detection methods [also] include software solutions, specifically, software intrusion detection systems, which continually monitor network traffic and look for known patterns of attack (1:19-32).” Shanklin continues by disclosing the dynamic portion of the system in the recitation, “signatures are stored, and, in real time, compared, to the packet flow incoming to the network. If a match is found, the incoming datastream is assumed to be misused (1:38-42).”

The Examiner further submits that the Applicant argument regarding the Examiner’s supposed equating of Shanklin’s session-based and packet-based load balancing with “receiving a monitoring policy and a plurality of monitoring points to be monitored on a network with any of said network intrusion detection systems” is not correct. The Examiner clarifies that the Office Action dated August 5, 2008 clearly states, "the Examiner directs the Applicant to column 2 lines 1-13 in which Shanklin et al. discloses the claimed “monitoring policy” as being inclusive to the IDS sensors, which comprise: ‘packet load to the sensors that is ‘load balanced,’ such that said packets are distributed at least at a session-based level [or] packet based level … the results of the detection performed by the sensors and the network analyzer are used to determine if there is an attempt to gain unauthorized access to the network.’” This disclosure corresponds with the citation of Shanklin noted above, in which the device for monitoring network activity or the IDS is configured by the administrator of the local network based on the enterprise's security policy. The Examiner is clarifying that the monitoring or "security policy" disclosed by Shanklin, that is provided by the administrator and is configured into each monitoring device or sensor (thus making it inclusive to the sensor) is what is being equated to the claimed and argued, "receiving a monitoring policy and a plurality of monitoring points to be monitored on a network with any of said network intrusion detection system."

Base upon the above reasoning the Examiner maintains the rejection.

**(11) Related Proceeding(s) Appendix**

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/C. C. O./

Examiner, Art Unit 2436

Conferees:

Nasser Moazzami

/Nasser G Moazzami/

Supervisory Patent Examiner, Art Unit 2436

Kambiz Zand

/Kambiz  Zand/

Supervisory Patent Examiner, Art Unit 2434